

# Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme

Linning Peng, *Member, IEEE*, Aiqun Hu, Junqing Zhang, Yu Jiang, Jiabao Yu, and Yan Yan

**Abstract**—Radio frequency (RF) fingerprint is the inherent hardware characteristics and has been employed to classify and identify wireless devices in many Internet of Things (IoT) applications. This paper extracts novel RF fingerprint features, designs a hybrid and adaptive classification scheme adjusting to the environment conditions, and carries out extensive experiments to evaluate the performance. In particular, four modulation features, namely differential constellation trace figure (DCTF), carrier frequency offset, modulation offset and I/Q offset extracted from constellation trace figure (CTF), are employed. The feature weights under different channel conditions are calculated at the training stage. These features are combined smartly with the weights selected according to the estimated signal to noise ratio (SNR) at the classification stage. We construct a testbed using universal software radio peripheral (USRP) platform as the receiver and 54 ZigBee nodes as the candidate devices to be classified, which are the most ZigBee devices ever tested. Extensive experiments are carried out to evaluate the classification performance under different channel conditions, namely line-of-sight (LOS) and non-line-of-sight (NLOS) scenarios. We then validate the robustness by carrying out the classification process 18 months after the training, which is the longest time gap. We also use a different receiver platform for classification for the first time. The classification error rate is as low as 0.048 in LOS scenario, and 0.1105 even when a different receiver is used for classification 18 months after the training. Our hybrid classification scheme has thus been demonstrated effective in classifying a large amount of ZigBee devices.

**Index Terms**—Physical layer security, RF fingerprint, device classification, Internet of Things

## I. INTRODUCTION

THE ubiquitous connections have significantly transformed our everyday life by connecting people, machine, and environment together through a wireless manner, which have triggered many exciting Internet of Things (IoT) applications such as smart city, smart healthcare, intelligent transportation etc. [1]–[3]. Identity authentication is essential in wireless communications to validate whether the users are legitimate, which is conventionally maintained by classical cryptography-based authentication techniques [4]. These schemes usually employ IP or MAC addresses as the identity,

which can be tampered or attacked [5]. In addition, cryptographic algorithms usually rely on complicated mathematical operations or protocols [6], while many IoT devices are low cost and sensitive to computational complexity. Take industrial IoT applications, such as environmental monitoring as an example. A star network topology is very suitable to connect low cost devices [7], where a host is usually employed to collect data from sensors. These sensors could be scattered in a vast field and will have to work for many years (e.g., ten years) with non-rechargeable batteries. While the host needs to authenticate the information source, it is very challenging for the sensors to support complex cryptography-based authentications with the limited energy. It is also not practical to update the pre-shared key or algorithm in these sensors. Therefore, a lightweight authentication and identification solution is urgently needed for the IoT.

Radio frequency (RF) fingerprint is an inherent characteristic of wireless device itself and can hardly be changed [8]–[11]. Similar to the human fingerprint, the RF fingerprint can be adopted to identify and classify wireless devices, which has been an emerging technique for wireless security. The RF fingerprint-based identification usually consists of two stages, namely the training and classification. At the training stage, the host receiver will first sample received signals from the devices under good channel quality, extract features, and save them as a template for reference. During the classification stage, the receiver will obtain signals from candidate devices, compare the same type features with the template, and classify the devices based on the similarity between these features. The RF fingerprint is inherently affiliated at the transmitted signal of the end devices, which does not cost any additional energy. On the other hand, the host is usually equipped with sufficient computational resources, which is capable to identify devices according to various RF fingerprint features residing in the received signals. The asymmetry of the computational resources and capabilities among host and end devices are very common in the IoT. Because the RF fingerprint identification does not require complicated mathematical operations from the end devices, it is extremely suitable to IoT. Therefore it has been reported with many prototypes and applications among various wireless systems, including UWB [12], GSM [13], LTE [14], WiFi [15]–[18], ZigBee [19]–[23], Bluetooth [24], RFID [25], wireless audio communications [26], and so on.

Feature extraction determines the type of RF fingerprint that can be used for classification. The state-of-the-art RF fingerprint-based identification methods can be generally summarized into three categories, namely transient-based techniques, spectrum-based techniques, and modulation-

Manuscript received xxx xxx, xxxx; revised xxx xxx, xxxx.

This work was supported in part by the National Natural Science Foundation of China under Grant 61571110, 61601114, 61602113, Natural Science Foundation of Jiangsu Province under Grant BK20160692 and CALT Fund.

L. Peng, A. Hu, Y. Jiang, and J. Yu are with the School of Cyber Science and Engineering, Southeast University, No.2 Sipailou, Nanjing, China. (email: {pengln, aqhu, jiangyu, yujiabao}@seu.edu.cn).

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk).

Y. Yan is with China Academy of Launch Vehicle Technology. (email: yan\_nj@163.com).

based techniques. The transient-based methods measure the turn-on/off transient or transmitting RF signal variations for device identification<sup>1</sup>, e.g., the envelope of the transient signal [15], [18], [20], [22]–[24] and the phase offset [27]. However, this method is extremely sensitive to the device position and antenna polarization direction [28], which limits the practical implementations. Moreover, high performance equipments with good receiver sensitivity and linearity, e.g., oscilloscope and spectrum analyzer, are essentially required to extract transient features from the received signal [19], [20], [28], [29], which significantly increases implementation cost. Low-cost equipments such as universal software radio peripheral (USRP) may compromise the classification performance [17], [30]. Signal spectrum is another important device fingerprint feature, e.g., received signal spectrum of 802.11 WiFi devices [17], [31], power spectrum density (PSD) of RFID tags or UWB devices [25], [32]. However, the performance of spectrum-based identification may deteriorate when channel condition changes [33]. In particular, when the receiver signal to noise ratio (SNR) decreases, the background noise will submerge signal PSD. Modulation-based methods extract stable features from the received signal, including auto gain control (AGC) responds [34], amplifier nonlinearity characteristics [35], sampling frequency offset [36], carrier frequency offset [36]–[41], distance vector [14], etc. These modulation-based features can be extracted in the baseband by using low cost devices, such as USRP. It is interesting to investigate these features and further integrate lightweight authentication in baseband signal processing.

Classification algorithm design is another key aspect of the RF fingerprint-based identification, which defines the methodology to classify the devices based on the extracted features. The classifier can be equipped with advanced tools such as artificial neural networks (ANN) and support vector machines (SVM) [20], which, however, may require a sophisticated training process. Statistical approaches including multiple discriminant analysis (MDA) [20] and linear discriminant analysis (LDA) [40] are also adopted but Gaussian distribution liked input features are assumed which may not always be valid [20]. Multiple features can be combined to improve the classification performance [16], [36]. For example, the work in [36] can achieve a classification rate of 47% by combining five features together with 93 candidate WiFi devices. On the other hand, the best classification rate is 26% when only one single feature is used. However, the performance is far from making a reasonable and meaningful decision, which is partly because only a simple linear combination of these features is used [16], [36]. A lightweight yet effective classifier combining multiple features in a smarter way is urgently required.

Finally, more comprehensive experimental investigations are required to demonstrate and validate the feasibility and robustness of RF fingerprint-based identification. Many prototype systems only involve a limited number of test devices, usually less than 10, for evaluations. For example, only six devices are tested in [30]. There are efforts to increase the test samples but the performance is not satisfactory. For example, the work

in [36] tries to classify 93 WiFi devices but the error rate is as high as 53%. In addition, the experiments are extremely sensitive to environmental conditions, including the presence of line-of-sight (LOS) or different emitter locations [28], [33], [42]. Moreover, the training and classification usually will not be carried out at the same time period or with the same receiver. For example, the training set can be provided by the manufacturer of the hardware devices as a database to the customers who will have to use another receiver platform for classification. The evaluation in [36] spans over three weeks, which are not long enough. More investigations under these circumstances are thus essential to demonstrate that RF fingerprint-based identification is applicable.

This paper proposes a hybrid device classification scheme based on multiple RF fingerprint features to classify ZigBee devices and carries out extensive experiments to evaluate the performance. In particular, we employ four modulation features, namely differential constellation trace figure (DCTF), carrier frequency offset, modulation offset and I/Q offset extracted from constellation trace figure (CTF). We also design a hybrid classifier scheme to adaptively combine different features according to the channel SNR. A testbed is constructed by a low-cost USRP software defined radio (SDR) platform as the host receiver and 54 CC2530 ZigBee nodes as the target devices to be classified, which are the most ZigBee devices ever tested. Compared to other existing work, we carry out much more extensive experiments to investigate the classification performance under different channel conditions, different experiment time and two receiver platforms, which is the first work to demonstrate the robustness of the RF fingerprint features with such experimental conditions. The contributions of this paper are summarized as follows.

- We propose to extract novel RF fingerprint features. DCTF is a new feature that can be obtained using differential of the received signals and processed by image recognition algorithms. Frequency offset is found to be distinguishable even at very low SNR but with slight variations at different measurements. Finally, CTF contains detailed information of the modulation offset and I/Q offset. These four features are proved to be very effective for classifications.
- We design a hybrid classifier by adjusting feature weights according to the channel conditions. The weights are pre-calculated with different channel SNR during the training stage. The corresponding weights are selected for classification based on the estimated SNR. To the best of the authors' knowledge, this is the first classifier integrating RF fingerprint features with weights adjusted adaptively according to channel conditions.
- We evaluate our proposed method with extensive experiments and demonstrate the robustness against channel conditions, experimental time and receiver platforms. We verify the performance under both LOS scenario and non-line-of-sight (NLOS) scenario, with a classification error rate of 0.0488 and 0.0941, respectively. We carry out classification experiments 18 months after the training with the same receiver, which is the longest time

<sup>1</sup>We use identification and classification interchangeably in this paper.

TABLE I  
NOTATIONS USED THROUGHOUT THE PAPER

Notation	Definition
$y(t)$	Received signal
$d(t)$	Signal after differential process
$\lambda$	Differential interval for DCTF
$\varepsilon$	I/Q phase mismatch distortion for DCTF
$\Phi_{M,N}$	Measurement matrix from DCTF
$\Omega_{M,N}$	Sensing matrix
$\Gamma_l$	The $l^{th}$ mean of points in $\Omega_{M,N}$
$\vec{\Gamma}$	Vector of clustering centers from DCTF
$\widehat{\Delta f}_{coarse}$	Estimated coarse frequency offset
$\widehat{\Delta f}_{fine}$	Estimated fine frequency offset
$\widehat{\Delta f}$	Estimated total frequency offset
$\widehat{\psi}$	Estimated phase offset
$\chi_n$	Fan-shaped section in CTF
$N_\chi$	Number of the fan-shaped sections
$N_{\chi_n}$	Number of received samples in each section $\chi_n$
$C_{\chi_n}$	Average center of samples dropped into the $\chi_n$
$\vec{R}$	Vector of CTF distortion
$(M_I, M_Q)$	Estimated I/Q offset from CTF
$\vec{\Theta}$	Feature group
$\gamma$	SNR
$\eta$	Intra-class variance
$\xi$	Inter-class variance
$\zeta$	Ratio between intra-class and inter-class variances
$\omega_p^\gamma$	Weight of $p^{th}$ feature at SNR $\gamma$

gap reported, and the error rate is only a little worse, increasing to 0.0546. We use a different receiver for classification for the first time and the error rate is 0.1105. The performance is much better than other work.

The DCTF-based RF fingerprint identification method is first proposed in our previous work [43]. This paper significantly extends by proposing a hybrid classifier integrating multiple RF fingerprint features, and performing a much more extensive experimental validation.

The notations and their definitions used in this paper are summarized in Table I. The remainder of this paper is organized as follows. Section II introduces the experimental system. Section III presents RF fingerprint features and their extractions and Section IV designs a hybrid ZigBee device classification approach. Experimental results are presented in Section V and Section VI concludes the paper.

## II. EXPERIMENTAL SYSTEM

ZigBee is widely used in wireless personal area network with popular IoT applications [44], including health-care [45], sensor networks [46] and vehicle-to-vehicle communications [47]. The ZigBee protocol uses the IEEE 802.15.4 as the physical layer technique, in particular, the Offset-QPSK (OQPSK) modulation [48]. The preamble consists of 32-bit zeros, which is used for synchronization. It uses direct-sequence spread spectrum (DSSS) coding and the chip length  $N_{chip} = 32$  when the system runs at 2.4 GHz.

The experimental system is shown in Fig. 1, which works at 2.4 GHz industrial, scientific and medical (ISM) band. We aim to classify 54 TI CC2530 ZigBee modules. USRP platforms with daughterboards UBX are used as receivers for capturing RF signals with a sampling rate of 10 Msample/s [49]. We sample 120 symbols of the physical layer waveform, which

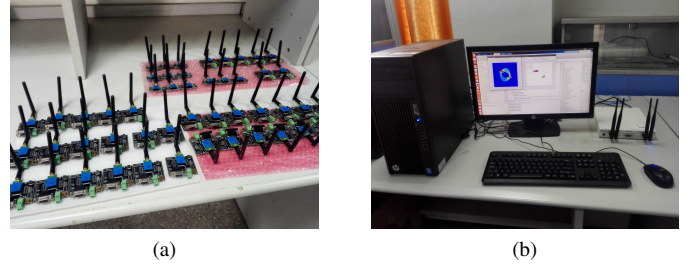


Fig. 1. (a) Photo of 54 target ZigBee devices. (b) Photo of the USRP receiver platform and PC.



Fig. 2. Feature extraction from DCTF

are used to extract RF fingerprint features in this paper. The captured baseband signal from USRP is transferred to a PC and processed off-line.

## III. RF FINGERPRINT FEATURES EXTRACTION

In this section, we introduce the extraction of the employed RF fingerprint features, including (i) DCTF, (ii) frequency offset, and (iii) CTF features.

### A. Differential Constellation Trace Figure Feature

DCTF method plots the differential signals in an I/Q axis and then employs image processing algorithms to extract the unique feature of RF signals in terms of different gathering centers. The flow chart of DCTF extraction is shown in Fig. 2. A differential process at the receiver is first carried out, which is given as

$$d(t) = (y_I(t) + jy_Q(t + \varepsilon)) \cdot (y_I(t + \lambda) + jy_Q(t + \lambda + \varepsilon))^*, \quad (1)$$

where  $y_I(t)$  and  $y_Q(t)$  are the received baseband signals at I/Q channels,  $\lambda$  is the differential interval,  $\varepsilon$  is the introduced I/Q phase mismatch distortion, and  $(\cdot)^*$  denotes the conjugation operation. As shown in (1), a small I/Q phase mismatch distortion  $\varepsilon$  is deliberately added to enlarge the RF fingerprint features in DCTF [43]. A delayed version of received signal is created by adding the differential interval  $\lambda$ . The differential process is then carried out by a conjugate multiplication between the received signals and their delayed copies. The obtained samples after differential process are directly depicted in an I/Q axis figure, which is named as DCTF.

We can then use image processing algorithms to analyze the features of the DCTF. The original DCTF is set as  $M \times N$  dimension pixel grids. The number of received signal samples in the pixel  $(m, n)$  is denoted as a measurement matrix  $\Phi_{m,n}$ , which is shown in Fig. 3(a). In order to efficiently extract features, the measurement matrix is converted to a sensing matrix with only two-level quantization. A sensing matrix  $\Omega_{M,N}$  is adopted and defined as

$$\begin{cases} \Omega_{m,n} = 1, & \Phi_{m,n} \geq \alpha \\ \Omega_{m,n} = 0, & \Phi_{m,n} < \alpha \end{cases}, \quad (2)$$

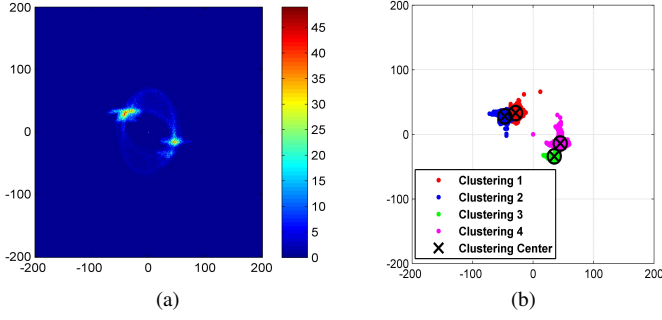


Fig. 3. (a) Obtained DCTF of ZigBee device,  $\lambda$  is 1 symbol length and  $\varepsilon$  is 1/10 symbol length. (b) Clustering centers from DCTF,  $N_L = 4$  and  $\alpha = 6$ .

where  $\alpha$  is the threshold and selected according to the size of  $M \times N$ , number of samples, and noise level. For instance, the chance of different samples falling into the same pixel will be lower when the size  $M \times N$  is larger. In addition, more samples will be in each pixel when there are more measurement samples. The noise will also fuzz the pixels with highly concentrated samples. In this paper, the threshold  $\alpha$  is selected as 6 after a few trying.

The point density of each pixel is an intuitive fingerprint which can represent the distortions of the wireless device. As shown in Fig. 3(b), the I/Q phase mismatch causes  $N_L = 4$  different clustering region centers,  $\Gamma_l$ , for Zigbee OQPSK modulated signals. A detailed derivation can be found in our previous work [43]. The k-means clustering algorithm uses least squared Euclidean distance to find the nearest mean, which is an efficient machine learning algorithm to get the clustering centers. As the clustering region number is fixed at 4 for OQPSK modulation and the number of pixels for clustering on DCTF is small, the k-means clustering is very suitable because of its easy implementation and low complexity. Finally, the receiver obtains a feature vector of clustering centers  $\bar{\Gamma} = \{\Gamma_l\}$  for classifications.

DCTF has demonstrated to be effective to distinguish different devices. An example of DCTFs of six ZigBee devices is shown in Fig. 4. As shown among the figures, the obtained DCTFs have significant differences among devices. DCTF-based classification can be achieved by image classification, which is a popular area of classical pattern recognition. In this paper, the k-means clustering algorithm is adopted as an example and advanced pattern recognition techniques can be employed to improve the performance.

### B. Frequency Offset Feature

Carrier frequency offset results from the different oscillator frequencies at the transmitter and receiver, which is also a popular parameter for device classification. In this paper, we introduce an accurate frequency offset estimation method to classify ZigBee devices. The estimated frequency offset information can be further used to extract the modulation offset feature in Section III-C. A block diagram of ZigBee frequency offset feature and modulation offset feature extraction is shown in Fig. 5.

1) *Coarse Frequency Offset Estimation*: There is a preamble sequence in the beginning of the ZigBee packet, which

can be used to estimate coarse frequency offset. The OQPSK waveform of the preamble sequence,  $z(n)$ , is first pre-calculated. A sequence correlation window is selected and frequency pre-compensation is performed by step-by-step frequency searching, i.e.,  $\hat{\Delta f}_{\text{coarse}} = f_{\text{start}} + f_{\text{step}}$ . Finally, the frequency offset incurring the correlation peak is selected as the coarse frequency pre-compensation value. The process is mathematically given as

$$\arg\max_{\hat{\Delta f}_{\text{coarse}}} \sum_{n=1}^{N_{\text{preamble}}} |y(t + nT_s) \cdot e^{-j2\pi\hat{\Delta f}_{\text{coarse}}nT_s} \cdot z^*(n)|, \quad (3)$$

where  $N_{\text{preamble}}$  is the length of the preamble sequence waveform, and  $T_s$  is the sampling rate.

2) *Fine Frequency Offset Estimation*: Due to the spread spectrum technique used in the ZigBee systems, transceiver can carry out the communication successfully even with slight carrier frequency offset. Therefore, very few algorithms have been proposed for ZigBee fine frequency offset estimation. However, we aim to get a more accurate estimation of carrier frequency offset in order to improve the classification accuracy.

The received signal is firstly compensated with the coarse frequency offset, which can be given as

$$y'(t) = y(t)e^{-j2\pi\hat{\Delta f}_{\text{coarse}}t}. \quad (4)$$

A peak correlation value is obtained by means of the cross-correlation between the compensated signal  $y'(t)$  and the known OQPSK spread spectrum chips  $z_i(n)$ , which is mathematically given as

$$\arg\max_i \sum_{n=1}^{N_{\text{chip}}} |y'(N_{\text{chip}} \cdot (k-1)T_s + nT_s) \cdot z_i^*(n)|, \quad (5)$$

where  $k$  is the index of ZigBee symbol. For IEEE 802.15.4 standard, there are 16 spread spectrum chips in total.

The chip index returned by (5) is denoted as  $i_{\text{corr}}$ . We then construct a signal  $s(k)$  as

$$s(k) = \sum_{n=1}^{N_{\text{chip}}} y'(N_{\text{chip}} \cdot (k-1)T_s + nT_s) \cdot z_{i_{\text{corr}}}^*(n). \quad (6)$$

The differential value between adjacent  $s(k)$  can be given as

$$d(k) = s(k) \cdot s^*(k+1). \quad (7)$$

Finally, we can get the fine frequency offset estimation  $\hat{\Delta f}_{\text{fine}}$  as

$$\hat{\Delta f}_{\text{fine}} = \text{angle}\left(\frac{1}{K-1} \sum_{k=1}^{K-1} d(k)\right) \cdot \frac{1}{2\pi N_{\text{chip}}T_s}, \quad (8)$$

where  $K$  is the number of total symbols in estimation. The total frequency offset of the received ZigBee signal is  $\hat{\Delta f} = \hat{\Delta f}_{\text{coarse}} + \hat{\Delta f}_{\text{fine}}$ .

Moreover, the phase offset can be estimated as

$$\hat{\psi} = \text{angle}\left(\frac{1}{K} \sum_{k=1}^K s(k) \cdot e^{-j2\pi\hat{\Delta f}_{\text{fine}}kN_{\text{chip}}T_s}\right). \quad (9)$$

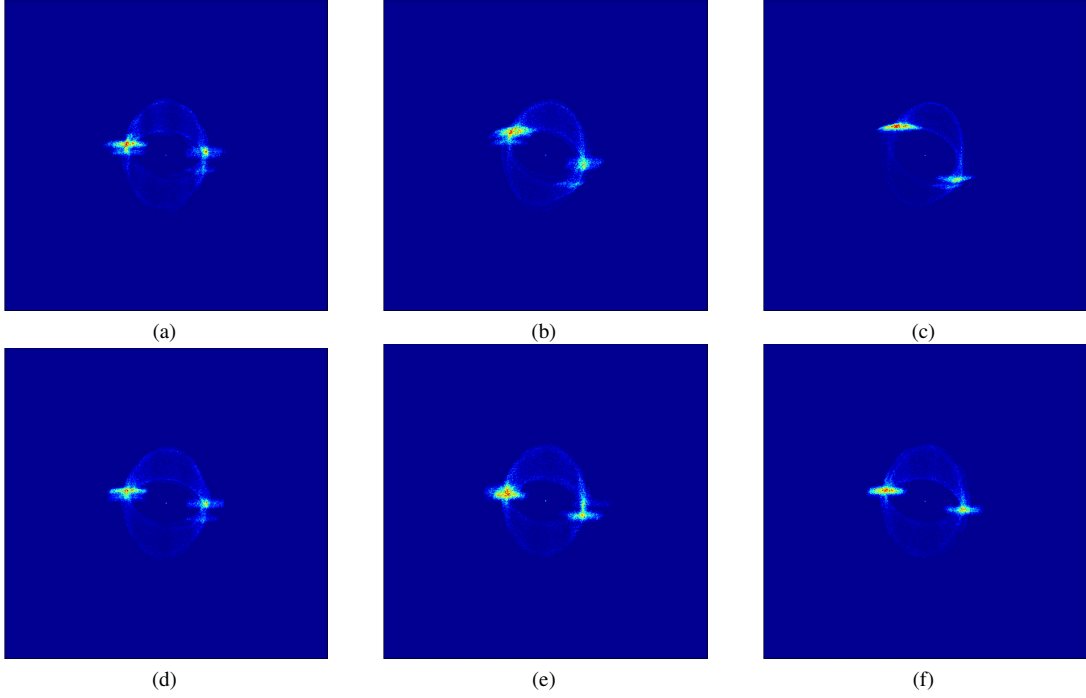


Fig. 4. Six DCTF fingerprints obtained from different ZigBee devices

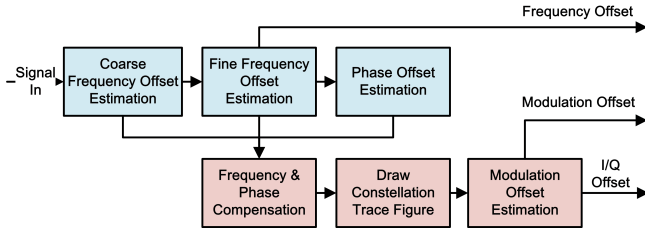


Fig. 5. Frequency offset feature and modulation offset feature extraction for ZigBee devices

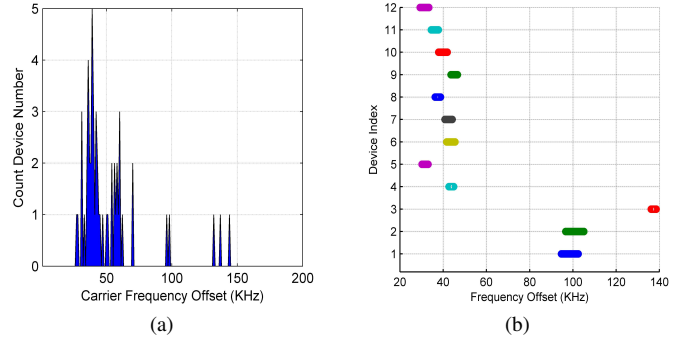


Fig. 6. (a) Frequency offset among 54 different ZigBee devices. (b) Frequency offset variations of the first 12 ZigBee devices.

The received ZigBee signal can be well compensated by the estimated frequency offset and phase offset.

We carried out the above frequency offset estimation to 54 different ZigBee devices and their frequency offsets are statistically shown in Fig. 6(a). Most of the devices have the frequency offset around 40 kHz while some of them have a frequency offset larger than 100 kHz. Furthermore, frequency offset is usually considered as a stable RF fingerprint feature for identifications and classifications [36]–[41], [50], [51], which may not be valid from our evaluation against working time. We find that the low-cost ZigBee devices have serious frequency offset variations even within 15 minutes evaluation. The frequency offset variations of the first 12 ZigBee devices are presented in Fig. 6(b). As shown in the figure, the range of the frequency offset variation varies from 5 kHz to 10 kHz. In addition, several devices have very similar frequency offset, e.g., the 4<sup>th</sup>, 6<sup>th</sup>, 7<sup>th</sup>, and 9<sup>th</sup> device. There will be a very high chance that different devices have similar frequency offset features, especially when there are many candidate devices. Therefore, it is not wise to only use frequency offset feature for classifications.

### C. Constellation Trace Figure Features

In practical systems, the amplifier non-linear behavior at the transmitter will severely distort the RF signal, which will cause non-linear signal offset at the receiver, including I/Q offset and phase offset. These features are usually extracted from the classical constellation map. However, constellation map only depicts the samples at the decision point, which can hardly illustrate the sample trace variations from one decision point to the next decision point. We deem that these trace variation is another important feature of wireless device. Therefore, we propose a new method termed as CTF to extract these features.

1) *CTF Plotting and Splitting*: We first compensate the received signal with the estimated frequency offset  $\hat{\Delta f}$  and phase offset  $\hat{\psi}$ , which is given as

$$y''(t) = y(t) \cdot e^{-j(2\pi\hat{\Delta f}t + \hat{\psi})}. \quad (10)$$

The CTF is obtained by directly plotting  $y''(t)$ , which is split into several sub-sections with following rules: (1) The base

point of the I/Q axis on CTF is set as a central point and (2) the CTF is equally split by a fixed angle from the central point. As a result, the CTF is split into several fan-shaped sections. For instance, we split the CTF into  $N_\chi = 8$  sections in Fig. 7(a). The  $n^{th}$  section is denoted as  $\chi_n$  and the number of received samples in  $\chi_n$  is  $N_{\chi_n}$ .

2) *Feature Extraction*: A measured average center  $C_{\chi_n}$  of all received samples dropped into the  $n^{th}$  section can be calculated as

$$C_{\chi_n} = \frac{1}{N_{\chi_n}} \sum_{i=1}^{N_{\chi_n}} y''(t_i)_{\chi_n}, \quad (11)$$

which can be further employed to extract the modulation offset features by the following two methods.

The first method extracts features from the obtained average central  $C_{\chi_n}$  values directly. As the received samples are normalized, the ideal average centers  $C_n$  of  $\chi_n$  can be calculated from simulations. In OQPSK,  $C_n$  is on the unit circle with different phases. The overall offset (CO) of the obtained CTF is calculated as the error vector at each average center, which is given as

$$\vec{R}_n = C_n - C_{\chi_n}. \quad (12)$$

The error vector  $\vec{R}$  represents the overall distortion of the obtained CTF. An illustration of ideal average center  $C_n$ , measured average center  $C_{\chi_n}$  and error vector  $\vec{R}_n$  are depicted in Fig. 7(b).

We can also obtain additional information from the average central  $C_{\chi_n}$  values. The CTF I/Q offset (IQO)  $(M_I, M_Q)$  can be estimated from the average center as

$$\begin{aligned} M_{I_n} &= \sum_{n=1}^{N_\chi} \left( C_{\chi_n} \cos \angle C_{\chi_n} \right), \\ M_{Q_n} &= \sum_{n=1}^{N_\chi} \left( C_{\chi_n} \sin \angle C_{\chi_n} \right), \end{aligned} \quad (13)$$

where  $\angle \cdot$  returns the angle of the variable. An illustration of obtaining CTF I/Q offset is depicted in Fig. 7(c). As the modulated OQPSK signal is symmetrical at both I/Q axis, the sum of I/Q offset  $(M_I, M_Q)$  should be 0 when the received ZigBee signal is perfect without any offset. However, in a practical system, the I/Q offset at the transmitter will affect each transmitted samples and result in an overall distortion. Therefore, the obtained results  $(M_I, M_Q)$  will contain the inherent offset features, which can be treated as a unique transmitter RF fingerprint.

Some results of CTF overall offset and I/Q offset are depicted in Fig. 8(a) and Fig. 8(b), respectively. As shown in the figures, the ZigBee devices can be clearly distinguished from the extracted overall offset and I/Q offset. In addition, the obtained features are very stable among different measurements.

In this subsection, we introduce two feature extraction methods from CTF. Although the concept of this processing is not complicated, the most significant advantage is that these processes can overcome serious noise distortions due to the

central limit theorem. In addition, these feature extraction methods could also be further extended to other modulation schemes with similar symmetrical characteristic.

#### IV. HYBRID CLASSIFICATION

We aim to improve the classification performance by integrating the four features discussed in the above section, namely clustering centers  $\vec{I}$ , frequency offset  $\widehat{\Delta f}$ , CTF overall offset  $\vec{R}$ , and I/Q offset  $(M_I, M_Q)$ . These features are grouped as

$$\vec{\Theta} = \{\Theta_1, \Theta_2, \Theta_3, \Theta_4\} = \{\vec{I}, \widehat{\Delta f}, \vec{R}, (M_I, M_Q)\}, \quad (14)$$

and combined using a hybrid classifier for an adaptive classification. The block diagram of our proposed hybrid classification is shown in Fig. 9.

##### A. Training and Classifier Setup

In the training stage, the receiver collects signals with very high SNR from target devices, which can be done by near-field measurements. The receiver will then extract RF fingerprint and save these features as a template,  $\vec{\Theta}^R$ .

We design a hybrid classifier with different feature weights against SNRs. As shown in Fig. 9, we first capture the training signals with very high received SNR. Additive white Gaussian noise (AWGN) with different power levels is added to the captured signals to emulate different SNR levels  $\gamma$ . RF fingerprint features,  $\vec{\Theta}^\gamma$ , will be extracted afterward and weights for different features will be calculated.

A typical classifier design usually involves using intra-class variances and inter-class variances [52]. We extend the classifier design to different SNRs. Monte Carlo simulations are carried out for each SNR in order to obtain accurate weights. The feature extracted from device  $k$  in the  $j^{th}$  simulation with SNR  $\gamma$  is given as  $\vec{\Theta}^\gamma(k, j)$ . The intra-class variance  $\eta_p^\gamma$  is given as

$$\eta_p^\gamma(k) = \frac{1}{N_d} \sum_{k=1}^{N_d} \frac{1}{J} \sum_{j=1}^J \left( \Theta_p^\gamma(j, k) - E_p^\gamma(k) \right)^2, \quad (15)$$

where  $E_p^\gamma(k) = \frac{1}{J} \sum_{j=1}^J \Theta_p^\gamma(j, k)$ ,  $J$  is the total simulation number, and  $N_d$  is the number of devices. Any device wishing to be classified by the host receiver will have to enroll its feature during the training stage, we therefore assume that the receiver is aware of the number of devices. The inter-class variance  $\xi_p^\gamma$  can be calculated by

$$\xi_p^\gamma = \frac{1}{N_d} \sum_{k=1}^{N_d} \left( E_p^\gamma(k) - \bar{E}_p^\gamma \right)^2, \quad (16)$$

where  $\bar{E}_p^\gamma = \frac{1}{N_d} \sum_{k=1}^{N_d} E_p^\gamma(k)$ . Then a ratio  $\zeta_p^\gamma$  is defined as

$$\zeta_p^\gamma = \frac{\frac{1}{N_d} \sum_{k=1}^{N_d} \eta_p^\gamma(k)}{\xi_p^\gamma}, \quad (17)$$

in order to demonstrate the noise influence to the RF fingerprint features. Finally, the weights  $\omega_p^\gamma$  for different features at SNR  $\gamma$  is given as

$$\omega_p^\gamma = \frac{\frac{1}{\zeta_p^\gamma}}{\sum_{p=1}^P \frac{1}{\zeta_p^\gamma}}, \quad (18)$$



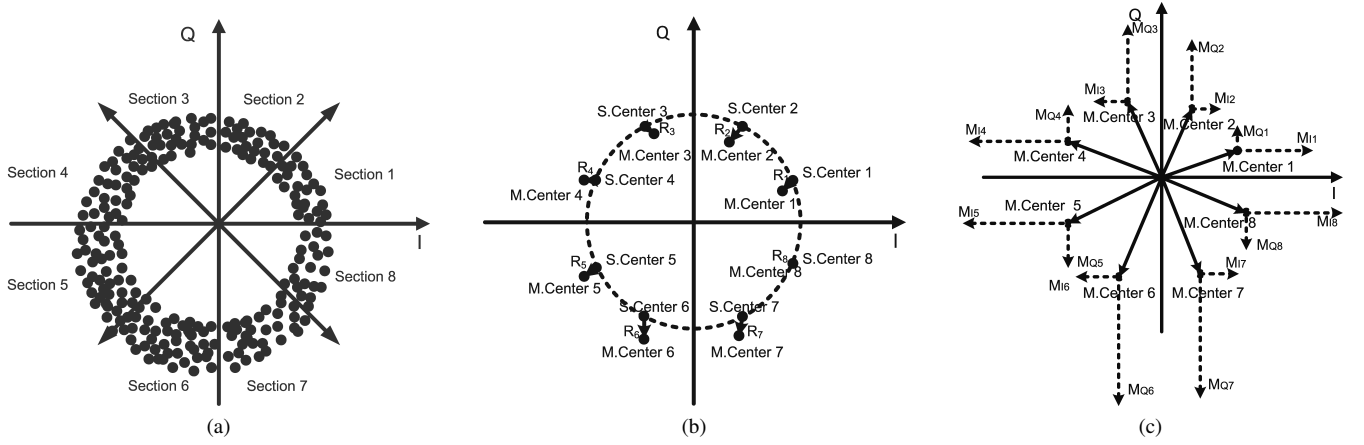


Fig. 7. (a) CTF plotting and splitting. (b) Obtaining error vector from CTF. (c) Obtaining I/Q offset from the CTF. S.Center means the ideal average center  $C_n$  and M.Center denotes the measured average center  $C_{\chi_n}$ .

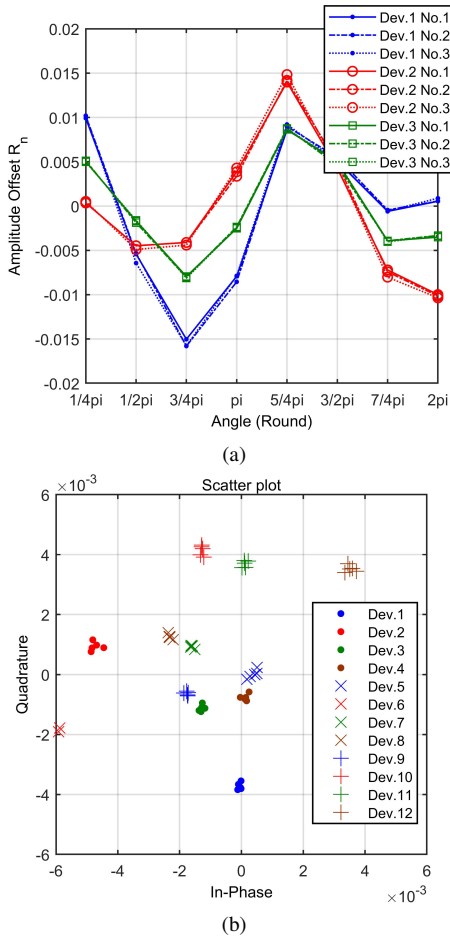


Fig. 8. (a) Overall offset among 3 different ZigBee devices with 3 measurements. (b) I/Q offset among 12 different ZigBee devices with 5 measurements.

where  $P$  is the number of total features, i.e.,  $P = 4$  in this paper.

### B. Classification

In the classification stage, the receiver will capture samples from the candidate devices to be classified, extract RF fingerprint features, and compare these features with the template

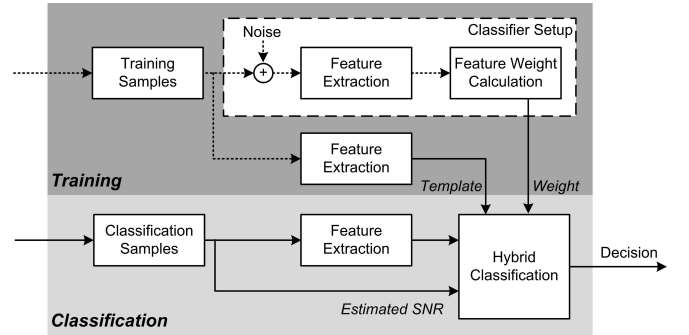


Fig. 9. Block diagram of hybrid classifier based on RF fingerprint

from the training stage. Different from schemes employing advanced classifier such as ANN, SVM, MDA [20], [40], a very lightweight classifier is introduced in our hybrid classification system. The receiver first estimates the received SNR,  $\hat{\gamma}$ , and extracts the features as  $\vec{\Theta}^{\hat{\gamma}}$ . It will then select the feature weights,  $\omega_p^{\hat{\gamma}}$ , calculated in the training stage. The distance between the features is calculated by comparing the obtained features,  $\vec{\Theta}^{\hat{\gamma}}$ , and the template features,  $\vec{\Theta}^R$ , then normalized and summed with feature weights. The index is returned by obtaining the minimum distance. The process can be mathematically given as

$$\operatorname{argmin}_{k_1, k_2} \sum_{p=1}^P \frac{|\Theta_p^{\hat{\gamma}}(k_1) - \Theta_p^R(k_2)|}{\xi_p^{\hat{\gamma}}} \omega_p^{\hat{\gamma}}. \quad (19)$$

When  $k_2 \neq k_1$ , a classification error occurs. The classification error rate  $\beta$  can be defined as

$$\beta = \frac{N_{\text{error}}}{N_{\text{test}}}, \quad (20)$$

where  $N_{\text{error}}$  is the number of classification error and  $N_{\text{test}}$  is the number of total tests.

## V. EXPERIMENTAL EVALUATION

### A. Hybrid Classifier Setup and Performance

The training processing was carried out in June 2016. We had 54 candidate ZigBee devices for classification. A USRP

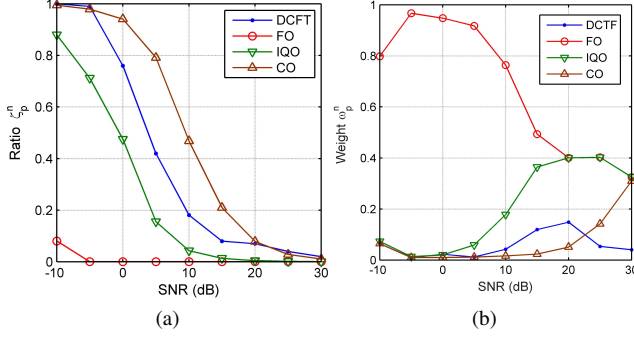


Fig. 10. (a)  $\zeta_p^\gamma$ , ratios between average intra-class variances and inter-class variances of each feature at different SNR. (b) Feature weights  $\omega_p^\gamma$  of each feature at different SNR.

X310 was used as a receiver to carry out the training process by collecting received signals from the 54 ZigBee devices, which were put very close to the receiver, with LOS between them. We simulated  $J = 2500$  times in order to obtain a reliable result. The ratio  $\zeta_p^\gamma$  and feature weights  $\omega_p^\gamma$  are calculated and shown in Fig. 10(a) and Fig. 10(b), respectively. The smaller the  $\zeta_p^\gamma$  is, the more reliable of this feature will be for classification. We can maintain a look-up table of feature weights  $\omega_p^\gamma$  against SNR  $\gamma$ .

The classifier performance under different SNR levels can also be evaluated through the setup process, which is shown in Fig. 11. The classification performance using individual feature can be calculated in a similar way to (19) and is shown in the figure as well. As shown in Fig. 11, classification using single feature varies greatly versus SNR, except the frequency offset. It is difficult to distinguish 54 ZigBee devices if only DCTF feature is used. In our previous work, DCTF-based feature extraction obtains quite good results, i.e., with a classification error rate as 10%, when there are only 16 ZigBee devices [43]. K-means clustering method is used at the moment but advanced pattern recognition algorithms can be adopted to improve the performance, which will be our future work. The performance of frequency offset-based classification is very stable even in low SNR scenario such as -5 dB. However, the classification error rate is always around 0.2, which is not satisfying. Modulation offset and I/Q offset from CTF are sensitive to SNR. The performance is quite good in high SNR environment but deteriorates dramatically when SNR is lower than 15 dB. Therefore, it is necessary to introduce adaptive features weights tuned to the SNR variations instead of fixed weights.

As shown in Fig. 11, the hybrid classification method achieves a significant performance enhancement. The classification error rate is less than 0.1 even at 5 dB SNR. This is because that the SNR affects feature estimation accuracy in a different manner. The feature weights are trained to the channel SNR, and the classification performance is improved by selecting the particular feature weights to integrate the features according to the estimated SNR. It is worth noting that the classifier weights are trained strictly following (18) without any manual intervention. In the low SNR scenario such as -10 dB, the hybrid method does not perform as well

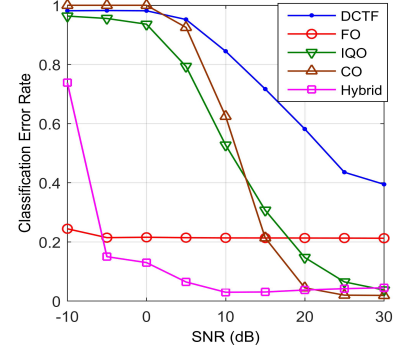


Fig. 11. Classification error rate of RF fingerprint classification using individual feature and our proposed hybrid classification method

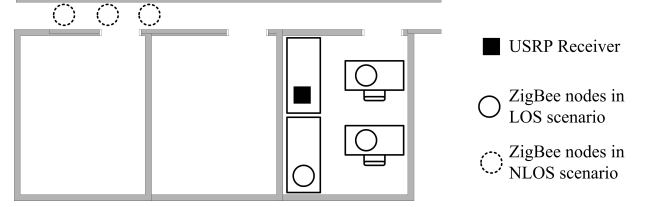


Fig. 12. Layout of the experimental environment

as the frequency offset-based method, because the increased inter-class variances of the estimated frequency offset reduce the frequency offset weight  $\omega_2^\gamma$  in Fig. 10(b). A more robust classifier can be designed by adjusting parameters manually, which will also be our future work.

We also did an empirical complexity evaluation of our system by calculating the execution time. A PC with Intel i7-4790, single thread at 3.6 GHz was used to count CPU time. We used Python 2.7 to build the USRP data control program and Matlab R2015b for data processing. It took approximately 560 ms for searching signal, SNR estimation and preprocessing, 840 ms for feature extraction and 50 ms for classification. Regarding the feature extraction, the execution time was 80 ms, 180 ms, and 580 ms for DCTF, frequency offset, and modulation and I/Q offset feature extractions, respectively. Although the complexity analysis is not rigorous, it demonstrates that the overall complexity of our algorithm is acceptable for practical implementations.

## B. Experimental Results

We carried out three experiments to evaluate the classification performance, namely robustness against channel conditions, experimental time, and receiver platforms. The layout of the experimental environment is shown in Fig. 12. For each device classification, we carried out five measurements by slightly moving the emitter in order to change channel conditions (SNR). Within each measurement, nine frame segments (each with 120 symbols) of ZigBee devices were obtained. We performed the classification algorithm using each collected frame segment and finally obtained approximately 45 classification results for each device.

The first classification experiment was carried out in June 2016, the same time period as the training process. Two



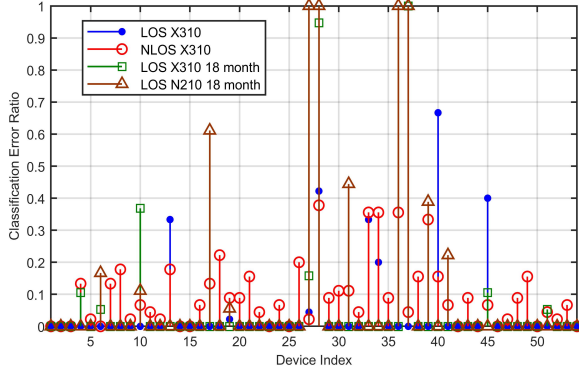


Fig. 13. Classification error rates of each device in different experiments

different channel conditions were considered, namely

- LOS scenario: The USRP X310 receiver and ZigBee devices were positioned in the same room. The distance between them was about 1-3 meters regarding different emitter locations.
- NLOS scenario: The USRP X310 receiver was positioned in a room and ZigBee devices were positioned in a long corridor outside the room. There was not a direct propagation line between USRP and ZigBee devices (blocked by the wall). The distance between the USRP and ZigBee devices was about 5-10 meters regarding different emitter locations.

The estimated SNR values of LOS and NLOS scenarios were around 20-25 dB and around 5-12 dB, respectively. The classification error rates of each device are presented in Fig. 13. As can be observed from the figure, the classification under LOS condition generally has a much better performance, which is reasonable because the SNR is much higher. We further calculated the total classification error rate, namely, the number of total false classifications divided by the number of total tests, which is 0.0448 in LOS scenario and 0.0941 in NLOS scenario.

The classification is usually not carried out at the same time with training stage. The RF fingerprint features may drift along time. Therefore, we carried out the second experiment in November 2017, i.e., 18 months after the training process, to test the time stability of the classification performance. The experiments were performed under a LOS condition and the same USRP X310 was used as the receiver. The results are shown in Fig. 13 and the total classification error rate is 0.0546, which is only a little worse. The RF fingerprint features are very stable for quite a long time.

Finally, we used another receiver to evaluate the performance when different receivers are used in the training and classification stages, which can be quite common. The experiments were also carried out in November 2017 under LOS condition but using a USRP N210 as the receiver. The results are shown in Fig. 13 and the total classification error rate is 0.1105, which is a little worse but still better than the performance of other work.

### C. Results Comparison

RF fingerprint-based identification has received many research interests. We compared our experimental results with other work, which is summarized in Table II and discussed in details as follows.

- Number of candidate devices: It is obvious that there is a higher chance to get a ‘collision’ in identification when more target devices are present. Most of the published work only verified their algorithms with less than 10 ZigBee target devices. We have investigated 54 ZigBee devices, which is the largest quantity of target devices. This preliminarily verifies the feasibility of RF fingerprint-based identification in practical IoT systems.
- Experiment environment condition: Most of other work evaluates their systems under a short distance LOS condition with the exceptions of the work in [33], [34]. However, the classification error rates are very high in their NLOS experiments even only 10 ZigBee devices are tested. We evaluated our system under both LOS scenario and NLOS scenario and both performances are good. In NLOS experiments, although only SNR degradation is considered in our hybrid classifier, our system outperforms other existing published NLOS experimental results. It is possible to introduce multi-path as another input of the hybrid classifier in order to further enhance the performance in NLOS scenarios.
- The number of used ZigBee symbols: It is intuitive that longer time will be taken to obtain sufficient samples when more symbols are required for identification. We only use 120 symbols in one ZigBee frame packet, which is the shortest compared to other work. This result demonstrates that the receiver could successfully distinguish the incoming packets only from their waveforms.
- Receiver platform: We only need low cost USRP as the receiver, while some classification systems may need sophisticated equipments, such as oscilloscope or Agilent E3238S signal monitoring system [20], [28]. In addition, this is the first work to carry out experiments with different receivers for training and classification stages. The classification error rate is 0.1105 when another USRP receiver is used from the training stage. This result could support the practical usage of RF fingerprint-based identification in real IoT environments.
- Template: Our system does not require the same environment to train the template and carry out the classification. However, some work does require that the received RF signals for classification and training are obtained exactly at the same place, termed as fixed template, which may not be practical for real experiments [28]. When changed template is used, i.e., RF signals for classification and training are obtained at different places, their system can hardly work [28].
- Stability: To the best of the authors’ knowledge, this is the first work that investigates the stability of RF fingerprint with 18 months time gap. The experimental results demonstrate that the RF fingerprint features remain stable over a long term, which is very suitable to

TABLE II  
COMPARISONS OF ZIGBEE DEVICE CLASSIFICATION VIA RF FINGERPRINT

Method	Number of Devices	Experiment Condition	Error Rate	Number of Symbols Used	Remark
Ours	54	1-3 m LOS	0.04	120	USRP
Ours	54	5-10 m NLOS	0.09	120	USRP
Ours	54	1-3 m LOS	0.05	120	18 month apart, same receiver
Ours	54	1-3 m LOS	0.11	120	18 month apart, different receiver
Knox <i>et al.</i> [34]	3	10 cm LOS	0	NA	
Patel <i>et al.</i> [20]	25	10 dB AWGN	0.1	3000	High cost
Patel <i>et al.</i> [30]	6	10 dB AWGN	0.1	1280	USRP
Dubendorfer <i>et al.</i> [22]	9	10 dB AWGN	0.1	1000	High cost
Ramsey <i>et al.</i> [23]	7	10 dB AWGN	0.1	500	High cost
Nguyen <i>et al.</i> [37]	4	NA	0	NA	USRP
Knox <i>et al.</i> [42]	5	1.5 m LOS	0.03	2000	USRP
Knox <i>et al.</i> [42]	5	4 m LOS	0.08	2000	USRP
Knox <i>et al.</i> [42]	5	10 m NLOS	0.19	2000	USRP
Boris <i>et al.</i> [28]	50	10 m LOS	0.03	600	Fixed template
Boris <i>et al.</i> [28]	10	40 m LOS	0.03	600	Fixed template
Boris <i>et al.</i> [28]	10	40 m LOS	0.38	600	Changed template
Wang <i>et al.</i> [33]	6	0.1 m LOS	0	1000	USRP
Wang <i>et al.</i> [33]	6	6 m NLOS	0.49	1000	USRP

IoT applications because they are designed to work for years.

#### D. Discussion

The experiments in this paper were carried out in a static setup, although with different distances. Many IoT networks may be mobile, e.g., vehicular communications. A Doppler shift of 133 Hz will be created when a car moves at a speed of 60 km/h and the carrier frequency is 2.4 GHz. However, it is much smaller compared to the ZigBee frequency offset estimated in this paper, ranging from 20 kHz to 140 kHz. In addition, the sampling time required for our identification is less than 5 ms. The channels are very similar during this period and the modulation parameters would probably remain the same. Finally, the movement will change the distance between the host receiver and the end devices, which will then affect the channel SNR and have been investigated thoroughly in this paper.

As RF fingerprint identification exploits features in the physical layer and its implementation is determined by the physical layer modulation. The feature extraction proposed in this paper does not apply directly to other wireless networks because of various physical layer modulations. For example, frequency offset also exists in other networks but they will adopt different estimation algorithms, e.g., short and long training symbols-based frequency offset estimation for IEEE 802.11 a/g/n/ac. However, the hybrid classifier should work with other networks, because the design methodology is applicable to any other multiple features-based classification. Finally, we have carried out extensive experiments, some of them are first performed in the RF fingerprint identification area. The experimental methodology of this paper offers a design guideline to evaluate the performance of any identification systems.

#### VI. CONCLUSION AND FUTURE WORK

This paper proposed a hybrid classification method by integrating novel RF fingerprint features in a smart manner and carried out extensive experiments to evaluate the performance. The contribution and novelty are three aspects. Firstly, four novel modulation-based features, namely DCTF, frequency offset, modulation offset and I/Q offset feature from CTF, were adopted and found effective in classifying ZigBee nodes. Secondly, a smart hybrid classifier was designed to adaptively integrating features with the weights tuned to the channel conditions. Finally, we constructed a testbed consisting of a low cost USRP SDR as the receiver platform and 54 ZigBee target devices, which were the most ZigBee devices tested. Compared to the existing work, much more extensive experiments were carried out to evaluate the feasibility and robustness of RF fingerprint-based identification under different channel conditions, experiment time, and receiver platforms.

Our hybrid device classification scheme has demonstrated good performances in various experiments. The total classification error rate was 0.0448 and 0.0941 under LOS scenario and NLOS scenario, respectively. The error rate was 0.0546 when the classification and training were carried out 18 months apart and the time gap is the longest among the literature to date. Finally, when a different receiver platform was used at the classification stage from the training stage, the error rate was 0.1105. It is the first time that a different receiver is used for classification to validate the robustness. Our classification performance is better than other reported ZigBee RF fingerprint-based classification schemes. The future work will focus on employing advanced pattern recognition algorithms to improve the DCTF classification accuracy and explore its applications in other physical layer modulated systems such as OFDM systems. We will also design a more robust and hybrid classifier by taking into account of channel influences

such as the multipath effect.

## REFERENCES

- [1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014.
- [2] S. Baker, X. Wei, and I. Atkinson, "Internet of things for smart healthcare: Technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26 521–26 544, 2017.
- [3] N. Lu, N. Cheng, N. Zhang, and X. Shen, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, 2014.
- [4] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.
- [5] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, 2014.
- [6] D. He and S. Zeadally, "An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, 2015.
- [7] "Application note, LoRa™ modulation basics," accessed on 19 April, 2018. [Online]. Available: <https://www.semtech.com/uploads/documents/an1200.22.pdf>
- [8] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, 2016.
- [9] P. Yu, G. Verma, and B. Sadler, "Wireless physical layer authentication via fingerprint embedding," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 48–53, 2015.
- [10] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 2016.
- [11] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys*, vol. 45, no. 1, pp. 1–29, 2012.
- [12] M. Kheir, H. Kreft, and R. Knchel, "UWB on-chip fingerprinting and identification using carbon nanotubes," in *Proc. IEEE Int. Conf. Ultra-Wideband (ICUWB)*, Paris, France, Sep. 2014, pp. 462–466.
- [13] M. D. Williams, M. A. Temple, and D. R. Reising, "Augmenting bit-level network security using physical layer RF-DNA fingerprinting," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Miami, USA, Dec. 2010, pp. 1–6.
- [14] F. Demers and M. St-Hilaire, "Radiometric identification of LTE transmitters," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Austin, USA, Dec. 2014, pp. 1–6.
- [15] H. Yuan and A. Hu, "Preamble-based detection of Wi-Fi transmitter RF fingerprints," *IET Electron. Lett.*, vol. 46, no. 16, pp. 1165–1167, 2005.
- [16] V. Briki, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. ACM Int. Conf. Mobile Computing Networking (MOBICOM)*, San Francisco, USA, Sep. 2008, pp. 116–127.
- [17] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," *IET Commun.*, vol. 8, no. 8, pp. 1274–1284, 2014.
- [18] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security," *J. Commun. Networks*, vol. 11, no. 6, pp. 544–555, 2012.
- [19] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1180–1192, 2015.
- [20] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Trans. Rel.*, vol. 64, no. 1, pp. 221–233, 2015.
- [21] B. W. Ramsey and B. E. Mullins, "Wireless intrusion detection and device fingerprinting through preamble manipulation," *IEEE Trans. Depend. Sec. Comput.*, vol. 12, no. 5, pp. 585–596, 2015.
- [22] C. K. Dubendorfer, B. W. Ramsey, and M. A. Temple, "An RF-DNA verification process for ZigBee networks," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Orlando, FL, USA, Oct./Nov. 2012, pp. 1–6.
- [23] B. W. Ramsey, M. A. Temple, and B. E. Mullins, "PHY foundation for multi-factor ZigBee node authentication," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Anaheim, USA, Dec. 2012, pp. 795–800.
- [24] J. Hall, M. Barbeau, and E. Kranakis, "Detecting rogue devices in bluetooth networks using radio frequency fingerprinting," in *Proc. Int. Conf. Commun. Comput. Networks (IASTED)*, Lima, Peru, Oct. 2006, pp. 108–113.
- [25] V. Lakafosis, A. Traillie, H. Lee, E. Gebara, M. M. Tentzeris, G. R. Dejean, and D. Kirovski, "RF fingerprinting physical objects for anti-counterfeiting applications," *IEEE Trans. Microwave Theory & Tech.*, vol. 59, no. 2, pp. 504–514, 2011.
- [26] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X.-Y. Li, "S2m: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, 2017.
- [27] D. A. Knox and T. Kunz, "Practical RF fingerprints for wireless sensor network authentication," in *Proc. Int. Wireless Commun. Mobile Computing Conf. (IWCMC)*, Cyprus, Aug. 2012, pp. 531–536.
- [28] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proc. Int. Conf. Inform. Process. Sensor Networks (IPSN)*, San Francisco, CA, USA, Apr. 2009, pp. 25–36.
- [29] T. J. Bihl, K. W. Bauer, and M. A. Temple, "Feature selection for RF Fingerprinting With Multiple Discriminant Analysis and Using ZigBee device emissions," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1862–1874, 2016.
- [30] H. Patel, M. A. Temple, and B. W. Ramsey, "Comparison of high-end and low-end receivers for RF-DNA fingerprinting," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Baltimore, USA, Oct. 2014, pp. 24–29.
- [31] S. U. Rehman, K. W. Sowerby, S. Alam, and I. Ardekani, "Portability of an RF fingerprint of a wireless transmitter," in *Proc. IEEE Int. Conf. Commun. Network Security (CNS)*, San Francisco, USA, Oct. 2014, pp. 151–156.
- [32] D. Ma, C. Qian, W. Li, and J. Han, "Geneprint: Generic and accurate physical-layer identification for UHF RFID tags," in *Proc. IEEE Int. Conf. Network Protocols (ICNP)*, Gottingen, Germany, Oct. 2013, pp. 1–10.
- [33] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2091–2106, 2016.
- [34] D. A. Knox and T. Kunz, "AGC-based RF fingerprints in wireless sensor networks for authentication," in *Proc. IEEE Int. Symp. on A World of Wireless Mobile and Multimedia Networks (WoWMoM)*, Montreal, QC, Canada, Jun. 2010, pp. 1–6.
- [35] G. Huang, Y. Yuan, X. Wang, and Z. Huang, "Specific emitter identification based on nonlinear dynamical characteristics," *Canadian J. of Elect. and Comput. Eng.*, vol. 39, no. 1, pp. 34–41, 2016.
- [36] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting Wi-Fi devices using software defined radios," in *Proc. ACM Conf. Security Privacy in Wireless and Mobile Networks (WiSec)*, Darmstadt, Germany, Jul. 2016, pp. 3–14.
- [37] N. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1404 – 1412.
- [38] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singele, and B. Preneel, "Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning," in *Proc. ACM Conf. Security Privacy in Wireless and Mobile Networks (WiSec)*, Boston, USA, Jul. 2017, pp. 58 – 63.
- [39] C. G. Wheeler and D. R. Reising, "Assessment of the impact of CFO on RF-DNA fingerprint classification performance," in *Proc. Int. Conf. Computing Networking and Commun. (ICNC)*, Santa Clare, USA, Jan. 2017, pp. 1–5.
- [40] H. Rahbari, M. Krunz, and L. Lazos, "Security vulnerability and countermeasures of frequency offset correction in 802.11a systems," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Toronto, Canada, Apr. 2014, pp. 1015–1023.
- [41] G. Zhang, L. Xia, S. Jia, and Y. Ji, "Identification of cloned HF RFID Proximity Cards Based on RF fingerprinting," in *Proc. IEEE Int. Conf. on Trust, Security and Privacy in Computing and Commun. (TrustCom)*, Tianjin, China, Aug. 2016, pp. 292 – 300.
- [42] D. A. Knox and T. Kunz, "Wireless fingerprints inside a wireless sensor network," *ACM Trans. Sensor Networks*, vol. 11, no. 2, pp. 37:1–37:30, 2015.
- [43] L. Peng, A. Hu, Y. Jiang, Y. Yan, and C. Zhu, "A differential constellation trace figure based device identification method for ZigBee nodes," in

- Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Yangzhou, China, Oct. 2016, pp. 1–6.
- [44] V. W. C. Chook, V. W. C. Chook, V. W. C. Chook, Y. F. Hu, Y. F. Hu, and Y. F. Hu, “Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards,” *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, 2007.
  - [45] J. Y. Jung and J. W. Lee, “Zigbee device design and implementation for context-aware U-Healthcare system,” in *Proc. Int. Conf. on Syst. and Networks Commun.*, Cap Esterel, France, Aug. 2007.
  - [46] H. Kdouch, G. Zaharia, C. Brousseau, and G. El Zein, “Zigbee-based sensor network for shipboard environments,” in *Proc. Int. Symp. Signals, Circuits and Syst.*, Lasi, Romania, Jun./Jul. 2011, pp. 1–4.
  - [47] C. Wang, C. Chou, P. Lin, and M. Guizani, “Performance evaluation of IEEE 802.15.4 nonbeacon-enabled mode for internet of vehicles,” *IEEE Trans. Intell. Transportation Syst.*, vol. 16, no. 6, pp. 3150–3159, 2015.
  - [48] *IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks*, IEEE Std., 2015, accessed on 19 April, 2018. [Online]. Available: <https://standards.ieee.org/findstds/standard/802.15.4-2015.html>
  - [49] “Ettus research,” accessed on 19 April, 2018. [Online]. Available: <http://www.ettus.com/>
  - [50] A. C. Polak and D. L. Goeckel, “Wireless device identification based on RF oscillator imperfections,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2492–2501, 2015.
  - [51] M. Pospisil, R. Marsalek, and J. Pomenkova, “Wireless device authentication through transmitter imperfections measurement and classification,” in *Proc. IEEE Int. Symp. Personal Indoor Mobile Radio Commun. (PIMRC)*, London, UK, Sep. 2013, pp. 497 – 501.
  - [52] S. Theodoridis and K. Koutroumbas, *Pattern Recognition*, 4th ed. Academic Press, 2009.